CLAIMS

What is claimed is:

1. A system for ensuring the legitimacy of a digital media file, the system comprising:

an analysis module for determining control information associated with the digital media file and for computing a known hash value that uniquely identifies the digital media file, thereby yielding an analyzed digital media file;

a storage operatively coupled to the analysis module, and for securely storing the known hash value and the control information associated with the analyzed digital media file;

a verification module operatively coupled to the storage and adapted to receive the analyzed digital media file, the verification module for computing a verification hash value from the analyzed digital media file received, and comparing that verification hash value to the known hash value; and

an outtake module adapted to transfer the analyzed digital media file in accordance with the associated control information in response to the verification hash value matching the known hash value.

2. The system of claim 1, wherein the analysis module further determines properties of the analyzed digital media file including at least one of file name, file size and file type, and stores those properties in the storage.

3. The system of claim 2, wherein the verification module compares at least one stored property of the analyzed digital media file with a corresponding actual property of the analyzed digital media file received.

4. The system of claim 1, wherein in response to the verification hash value not matching the known hash value, use of the analyzed digital media file is restricted.

5. The system of claim 1, wherein in response to the verification hash value not matching the known hash value, the verification module signals the analysis module to perform a reanalysis of the analyzed digital media file received.

6. The system of claim 1, wherein the analysis module determines the control information by performing a digital watermark screen.

7. The system of claim 1, wherein the control information includes usage rights associated with the digital media file.

8. The system of claim 1, wherein in response to no control information being associated with the digital media file, the analysis module assigns default usage rights to the digital media file.

9. The system of claim 1, wherein the determining of the control information and the computing of the known hash value are performed in parallel by the analysis module.

10. The system of claim 1, wherein the analyzed digital media file is stored unencrypted in the storage.

11. The system of claim 1, wherein the outtake module performs real-time encryption on the digital media file before transfer.

12. A system for verifying the legitimacy of a digital media file, the system comprising:

an analysis module for determining control information associated with the digital media file and for computing a known hash value that uniquely identifies the digital media file, thereby yielding an analyzed digital media file; and

a verification module adapted to receive the analyzed digital media file, and for computing a verification hash value from the analyzed digital media file received, and for comparing that verification hash value to the known hash value to verify the analyzed digital media file received has not been compromised.

13. The system of claim 12, wherein in response to the verification hash value not matching the known hash value, use of the analyzed digital media file is restricted.

14. The system of claim 12, wherein in response to the verification hash value not matching the known hash value, the verification module signals the analysis module to perform a reanalysis of the analyzed digital media file received.

15. The system of claim 12, wherein the analyzed digital media file is stored unencrypted in a storage.

16. The system of claim 12, further comprising:

an outtake module adapted to transfer the analyzed digital media file in accordance with the associated control information in response to the verification hash value matching the known hash value.

17. The system of claim 16, wherein the outtake module performs real-time encryption on the digital media file before transfer.

18. The system of claim 12, further comprising:

a storage operatively coupled to the analysis and verification modules, and for securely storing the known hash value and the control information associated with the analyzed digital media file.

19. The system of claim 12, wherein the system is contained on a computer readable medium in the form of software instructions.

20. A method for verifying the legitimacy of a stored digital media file previously established as legitimate, the method comprising:

retrieving the stored digital media file;

computing a verification hash value from the retrieved digital media file;

comparing the verification hash value to a known hash value previously associated with the stored digital media file as part of a comprehensive analysis in establishing the legitimacy of the digital media file; and

in response to determining that the verification hash value matches the known hash value, using the digital media file in accordance with control information associated with the digital media file.

21. The method of claim 20, wherein the control information is included in a digital watermark associated with the digital media file.

22. The method of claim 20, wherein the comprehensive analysis in establishing the legitimacy of the digital media file includes performing a digital watermark screen.

23. The method of claim 20, further comprising:

in response to the digital media file not being legitimate, restricting the use of the digital media file.

24. The method of claim 20, wherein the stored digital media file is unencrypted.

25. A method for verifying a digital media file previously established as legitimate has not been compromised, the method comprising:

running a predetermined hash function on the digital media file thereby computing a verification hash value;

determining if the verification hash value matches a known hash value previously associated with the digital media file;

in response to the verification hash value matching the known hash value, retrieving control information associated with the digital media file; and

using the digital media file in accordance with the control information.

26. The method of claim 25, wherein the digital media file is received from a database in response to a user request for that digital media file.

27. The method of claim 25, further comprising:

securely storing the known hash value associated with the digital media file.

28. The method of claim 25, further comprising:

securely storing usage rights defined by the control information associated with the digital media file.

29. The method of claim 25, further comprising:

in response to the verification hash value not matching the known hash value, reanalyzing the received digital media file.